ABSTRACT OF THE DISCLOSURE

A method and system for distributed network address translation with security features. The method and system allow Internet Protocol security protocol ("IPsec") to be used with distributed network address translation. The distributed network address translation is accomplished with IPsec by mapping a local Internet Protocol ("IP") address of a given local network device and a IPsec Security Parameter Index ("SPI") associated with an inbound IPsec Security Association ("SA") that terminates at the local network device. A router allocates locally unique security values that are used as the IPsec SPIs. A router used for distributed network address translation is used as a local certificate authority that may vouch for identities of local network devices, allowing local network devices to bind a public key to a security name space that combines a global IP address for the router with a set of locally unique port numbers used for distributed network address translation. The router issues security certificates and may itself be authenticated by a higher certificate authority. Using a security certificate, a local network device may initiate and be a termination point of an IPsec security association to virtually any other network device on an IP network like the Internet or an intranet. The method and system may also allow distributed network address translation with security features to be used with Mobile IP or other protocols in the Internet Protocol suite.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001